DEPARTMENT OF MENTAL HEALTH
POLICY/PROCEDURE

SUBJECT **CONFIDENTIAL AND SENSITIVE INFORMATION ON MICROCOMPUTER SYSTEMS**	POLICY NO. **302.9**	EFFECTIVE DATE **10/1/89**	PAGE **1 of 2**
APPROVED BY: **Original signed by:** **ROBERTO QUIROZ** Director	SUPERSEDES **103.1** **7/13/89**	ORIGINAL ISSUE DATE **7/13/89**	DISTRIBUTION LEVEL(S) **1**

PURPOSE

1.1 To ensure against the unauthorized release of and access to confidential patient and sensitive personnel information.

POLICY

2.1 All measures shall be taken to comply with all confidentiality laws, regulations, and policies.

2.2 All Department of Mental Health (DMH) policies on confidentiality and all legal requirements in relation to confidentiality shall be observed.

2.3 Only personnel who are authorized by DMH to have access to client information may request and receive confidential information. All requests shall be in compliance with all confidentiality laws, regulations, and policies.

2.4 Full confidentiality procedures shall be followed in regard to any reports with client identifying information. Plans for the storage and destruction of reports or forms must be in conformity with confidentiality procedures and be acceptable to the director responsible for the bureau, division, clinic, etc.

2.5 Access to output reports containing sensitive and confidential information shall be restricted to authorized personnel.

2.6 Destruction of outdated, sensitive or confidential output shall be controlled using shredders or secure recycling containers.

PROCEDURE

3.1 All microcomputer users are responsible for the following:

3.1.1 Complete and sign the Oath of Confidentiality, if not previously done.

3.1.2 Do not leave confidential or classified information on screen while the microcomputer is unattended or when processing has terminated.

3.1.3 Clearly mark information as “Confidential” or “Classified” on all data output/printouts and on storage diskettes or tapes.

3.1.4 Securely lock up sensitive or confidential data (disks, printouts, etc.) when not in use.

3.1.5 Do not store sensitive or confidential data on the microcomputer’s hard or fixed disk unless unauthorized access to the hard disk or data can be prevented, e.g., locking or disabling the central processing unit (CPU), encrypting/encoding of the data, using passwords to access the microcomputer or the data file.

AUTHORITY

Welfare and Institutions Code, Section 5330
County Fiscal Manual, Section 12.1.3